SECURITY MANAGEMENT DEVICE IN OPEN DECENTRALIZED ENVIRONMENT

Patent Number: JP7141296

Publication date: 1995-06-02

Inventor(s): SAITO YOKO

Applicant(s): HITACHI LTD

Requested Patent: ⌜ JP7141296

Application Priority Number(s): JP19930284990 19931115

IPC Classification: G06F15/00; G06F13/00;

EC Classification:

Equivalents:

Abstract

PURPOSE:To surely realize security management among domains (network system) A, B, and C having different kinds of equipment in a system in open decentralized environment.
CONSTITUTION:At an optional position in a network, a TTP (reliable 3rd party) for security management covering plural domains is provided, and a security policy setting and modifying means for the whole network NW1 and an access control decision means which controls and decide access covering plural domains according to the security policy are provided there. When there is requests to register security policies PA and PB from the domains A and B (managers MA and MB) (1), the TTB compares PA and PB from points of view of regulations of OSI such as certification, access control, and secrecy and absorbs differences in expression by mapping generate a security policy P which has no contradiction on the whole. On the basis of P, various security management such as access permission/inhibition decision making is performed.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－141296

(43)公開日　平成７年(1995)６月２日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ａ	7459－5L		
	13/00	３５１　Ｚ	7368－5B		
	15/16	４７０　Ｍ	7429－5L		

審査請求　未請求　請求項の数５　ＯＬ　（全 16 頁）

(21)出願番号　特願平5－284990

(22)出願日　平成５年(1993)11月15日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　齋藤　洋子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア開発本部内

(74)代理人　弁理士　武　顕次郎

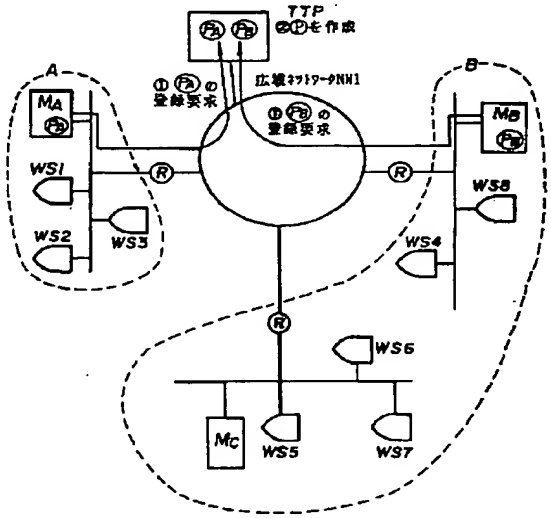
(54)【発明の名称】　オープンな分散環境におけるセキュリティ管理装置

(57)【要約】

【目的】　オープンな分散環境のシステムで、各々異機種を持つドメイン（ネットワークシステム）Ａ，Ｂ，Ｃ相互間でのセキュリティ管理を確実に実現する。

【構成】　ネットワーク上の任意の位置に、ドメイン間に跨がってセキュリティ管理をするためのＴＴＰ（信頼できる第三者）を設け、ここにネットワークＮＷ１全体のセキュリティポリシー設定及び変更手段や、このセキュリティポリシーに従ってドメイン間に跨がったアクセスを制御、判定するアクセス制御判定手段を設ける。ドメインA及びB（マネジャM_A，M_B）から各セキュリティポリシーP_A，P_Bの登録要求があると（①）、ＴＴＢはP_A，P_Bを、認証、アクセス制御、機密性等、ＯＳＩの規定での観点から比較し、表現の違いはマッピングにより吸収し、システム全体として矛盾のないセキュリティポリシーＰを作成する、このＰに基いてアクセス可否の判定等、色々なセキュリティ管理をする。

【図２】ＯＳＩ管理ドメイン間に跨がったセキュリティ管理モデル



1

【特許請求の範囲】

【請求項1】　ネットワークシステムを介して接続されたオープンな異機種の分散システム環境において、ネットワークシステム間に跨がったセキュリティ管理を行なうためのＴＴＰを設け、前記ＴＴＰに、ネットワークシステム全体のセキュリティポリシーを設定するセキュリティポリシー設定手段と、前記セキュリティポリシーを更新するセキュリティポリシー更新手段と、前記セキュリティポリシーの規定に従ってネットワークシステム間に跨がってアクセスを制御するアクセス制御手段とを備えたことを特徴とするオープンな分散環境におけるセキュリティ管理装置。

【請求項2】　前記ＴＴＰに、更に、前記ネットワークシステムに発生したセキュリティ侵害事象を収集、解析し警告を発するセキュリティ監査手段と、ネットワークシステム内の安全な通信の確保、データの完全性の保証及び認証のために必要な暗号鍵を管理する鍵管理手段と、ネットワークシステム内の通信の事実を保証するための否認不可保証手段とを備えたことを特徴とする請求項1記載のオープンな分散環境におけるセキュリティ管理装置。

【請求項3】　ネットワークシステムを介して接続されたオープンな異機種の分散システム環境において、ネットワークシステム間に跨がったセキュリティ管理を行なうためのＴＴＰを設け、このＴＴＰに、異なるネットワークシステムのオブジェクトを統合管理用オブジェクト及び関係属性を使用して定義してこの関係属性の定義情報を管理するオブジェクト管理手段と、前記異なるネットワークシステムのマネジャから他のネットワークシステムへのアクセス可否を決定するアクセス判定手段とを備えたことを特徴とするオープンな分散環境におけるセキュリティ管理装置。

【請求項4】　前記ＴＴＰに、更に、前記統合管理用オブジェクトと前記ネットワークシステムのマネジャのオブジェクトとの間に発生した不整合情報を調整するオブジェクト調整手段を備えたことを特徴とする請求項3記載のオープンな分散環境におけるセキュリティ管理装置。

【請求項5】　前記ＴＴＰが管理するセキュリティポリシーの規定に従って、暗号化、完全性及び否認不可に関するセキュリティ機能を実行させるアプリケーションプログラムインタフェースを提供したことを特徴とする請求項1ないし4のいずれか1記載のオープンな分散環境におけるセキュリティ管理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、オープンな分散環境におけるセキュリティ管理装置に係り、特に、オープンな異機種の分散環境において、ネットワークシステム間に跨がったセキュリティ管理を行なうことができるセキュリティ管理装置に関する。

2

【０００２】

【従来の技術】近年、ＥＤＩ（Electronic Data Interchange）やＥＦＴ（Electronic FundsTransfer）を始めとする電子取引が増加している。このようなネットワークを用いた取引では、取引自体に高度なセキュリティが要求されることは勿論のこと、異なる企業間のネットワークに跨がった接続が必要になるため、ネットワーク制御、管理が重要になる。ＬＡＮ（Local Area Network）やＷＡＮ（Wide Ares Network）を介した接続となると、ネットワーク資源の最大限の効果的な利用を図り、ネットワークの可用性（操作性、利用性）を向上させるため、単純イメージでの（個々のシステムを意識しない）管理システムが必要であるが、現在のところ、オープンな分散環境でどのようにセキュリティを考えればよいのかというモデルはまだ提案されていない。

【０００３】昨今、ネットワークシステムにおけるセキュリティについては、いろいろな機関でその重要性が叫ばれているにもかかわらず、未だに有効な解決策が提示されていない。例えば、ＩＳＯ（国際標準化機構：International Organization forStandardization）では、セキュリティアーキテクチャについてＳＣ２１／ＷＧ１で、鍵管理や暗号化アルゴリズムについてＳＣ２７／ＷＧ２で、システム管理面でのセキュリティについてＳＣ２１／ＷＧ４で、それぞれ検討されている。その各々は非常に意味ある重要な検討であるが、実装についてはうまくいっていない。現在セキュリティ機能が実装されているシステムでも、他システムと接続する際に新たにセキュリティ機能が必要になる。特に、セキュリティについては、システム管理者のポリシー（方針）に依存する部分が多く、また複数のネットワークを経由する場合にはその運用で決まる部分が多いので、これといった解決策が提案されていないのが現状である。しかし、今後オープンなネットワークシステムにおけるセキュリティが不可欠になってくるのは確実である。その時のために、オープンな分散環境での管理とセキュリティの解となるモデルを提案することは非常に重要であると考えられる。

【０００４】なお、セキュリティポリシー（安全保護方針）の概念は、ＯＳＩセキュリティフレームワークオーバビュー（ISO/IEC CD 10181-1）で規定されている。

【０００５】分散環境を考慮したセキュリティ技術としては、特開平４－３４２０５５号公報（文献1）や特開平４－３６７９５９号公報（文献2）及び特開平４－３６７９６０号公報（文献3）に記載された技術が知られている。文献1に記載された技術は、複数コンピュータシステムの利用者認証方法に関する発明であり、遠隔からのログオン時に遠隔利用者認証情報保持コンピュータ内の利用者認証情報を確認することにより、複数のコンピュータの持つ利用者認証情報を同一にする手間を不要

3

としている。また、文献2及び3に記載された技術は、ネットワーク管理システムに関する発明であり、この発明により、ネットワーク管理システムで、保守運用者に担当以外の局、装置に対する不正アクセスをさせないためのアクセス制御機能を提案している。

【0006】これらの発明は、いずれも1つのシステム内でのセキュリティ機能を実装しているが、他システムと接続する際に新たに必要になるセキュリティ機能については何も考慮していない。

【0007】

【発明が解決しようとする課題】上記文献1～3に記載された技術は、いずれも1つのシステム内でセキュリティ機能を実装したときのアクセス方法を開示しているだけであって、機種などの異なる他システムと接続する際に新たに必要となるセキュリティ機能については何も考慮されていない。

【0008】また、従来の技術のところでも少し触れたように、ISOの様々なWGでセキュリティモデルやサービス、サービスを実現するためのメカニズムが検討されているが、セキュリティに関する情報をどう管理するかは実装の問題とされている。OSI（開放型システム相互接続：Open Systems Interconnection）であればネットワークシステム内の情報はオブジェクト（管理対象）としてOSI管理によって管理され、OSI資源の取りまとめと制御のためにシステム管理の操作と層管理が提供されている。しかし、OSI管理では、「オープンシステム」での管理要件を定義しているのではなく自システム内で相互運用が発生した時の必要事項について定義しているだけであり、本質的な「オープンシステム」を扱っていない。つまり、OSI管理ではローカルシステムレベルの相互接続性のみが考慮され、個々のシステムは、他システムと管理情報の交換をしたり管理アクティビティ間を調整したりする「自己管理」（閉じられた中での管理）をしているシステムであると考えている。ところが、分散環境では、全てのシステムが自己管理されているとは限らないため、OSI管理のモデルでは分散環境に対応しきれない。これに対処するため、オープンな分散環境におけるセキュリティ管理モデルではこの部分（自己管理されていない部分）を補う必要がある。

【0009】また、OSI管理の情報DBであるMIB（Management Information Base）では、OSI環境で利用されるシステムでのデータ、及びOSIシステム間で管理情報の転送を行う時のサービスやプロトコルも定義されている。しかし、OSIでは、システムの管理アプリケーションにこれらのサービスを利用させるのに必要なAPI（Application Program Interface）については規定されていないので、ODP（Open Distributed Processing）のような高位なレベルでセキュリティ機能を定義する必要がある。特に、アプリケーションやシステム、ネットワーク間に跨がった視点からセキュリティを考え直すためには管理ソフトウェアに何が必要か考えることが必要であろう。

4

【0010】なお、本発明は、さきに特願平4－248059号の特許出願（以下、「先願1」という）において、1つのMOM（マネジャオブマネジャ）でサブシステム間の異種オブジェクトを統合管理する異種オブジェクトの統合管理方式を提案したが、この提案では、オープンな分散環境において、ネットワークシステム間に跨がった観点からセキュリティ管理することについてはなにも考慮していない。

【0011】以上の分散環境での管理とセキュリティの問題点から、オープン分散環境での管理とセキュリティの解となるモデルを実現するためには次の3点が必要であることがわかる。

【0012】①アプリケーションやシステム、ネットワーク間に跨がった視点からセキュリティを管理できること。

【0013】②「自己管理」されていないシステムでのオブジェクトの管理ができること。

【0014】③システムの管理アプリケーションに情報DBのサービスを利用させるAPI等の高位なレベルでのセキュリティ管理のオペレーションについて規定すること。

【0015】従って、本発明の目的は、上記従来技術の問題点を解決し、オープンな異機種の分散システム環境において、アプリケーションやネットワークシステム間に跨がってセキュリティを管理することができると共に、現状のネットワークシステムをセキュリティを損なうことなく容易に拡張することができ、自己管理されていないシステムでのオブジェクトの管理ができ、システムの管理アプリケーションに情報データベースのサービスを利用させるAPI等の高位なレベルで規定したオペレーションによるセキュリティ管理ができる、セキュリティ管理装置を提供することにある。

【0016】

【課題を解決するための手段】上記目的を達成するため、本発明は、ネットワークシステムを介して接続されたオープンな異機種の分散システム環境において、ネットワークシステム間に跨がったセキュリティ管理を行なうためのTTP（Trusted Third Party：信頼できる第三者機関）を設け、前記TTPに、ネットワークシステム全体のセキュリティポリシーを設定するセキュリティポリシー設定手段と、前記セキュリティポリシーを更新するセキュリティポリシー更新手段と、前記セキュリティポリシーの規定に従ってネットワークシステム間に跨がってアクセスを制御するアクセス制御手段とを備えたものである。また、このTTPに、前記ネットワークシステムに発生したセキュリティ侵害事象を収集、解析し警告を発するセキュリティ監査手段と、ネットワークシ

5

ステム内の安全な通信の確保、データの完全性の保証及び認証のために必要な暗号鍵を管理する鍵管理手段と、ネットワークシステム内の通信の事実を保証するための否認不可保証手段とを備えたものである。

【００１７】更に、このＴＴＰに、異なるネットワークシステムのオブジェクトを、統合管理用オブジェクト及び関係属性を使用して定義して、この関係属性の定義情報を管理するオブジェクト管理手段と、前記異なるネットワークシステムのマネジャから他のネットワークシステムへのアクセス可否を決定するアクセス手段とを備えたものである。また、このＴＴＰに、前記統合管理用オブジェクトと前記ネットワークシステムのマネジャのオブジェクトとの間に発生した不整合情報を調整するオブジェクト調整手段を備えたものである。

【００１８】更に、前記ＴＴＰが管理するセキュリティポリシーの規定に従って、暗号化、完全性及び否認不可に関するセキュリティ機能を実行させるアプリケーションプログラムインターフェースを提供するものである。

【００１９】

【作用】上記構成に基づく作用を説明する。

【００２０】本発明によれば、オープンな異機種の分散システム環境において、色々な機種をもつ複数のネットワークシステム間に跨がってセキュリティ管理を行なうために、ネットワーク上の任意の場所に、セキュリティ管理を行なうためのＴＴＰ（Trusted Third Party, JISのX5004参照）を設けたことを特徴としている。このＴＴＰ上で、セキュリティポリシーを設定登録しまた更新することにより、以下に分説するように、ネットワークシステム間に跨がって発生するアクセス要求に対するセキュリティ管理が容易に実現できる。

【００２１】（１）セキュリティポリシーの管理

各ネットワークシステムは、それぞれ一つのセキュリティドメインとして管理され、そのセキュリティドメイン内はセキュリティポリシーにより管理されている。しかし、セキュリティドメイン外の（他のセキュリティドメインの）エンティティから通信要求されてきた場合には、当該エンティティとの通信を認可するメカニズムが必要となる。本発明では、ＴＴＰを設けて、ここに、セキュリティポリシーの設定／更新操作及びドメイン間にまたがるアクセスの制御手段を備えたことにより、アプリケーションやシステム、ネットワーク間に跨がった視点からセキュリティが管理できる（図４，図５）。また、セキュリティ監査手段によりネットワークシステム（セキュリティドメイン）間に発生したセキュリティ侵害事件を収集解析して警告を発生し、鍵管理手段によりセキュリティドメイン内の安全な通信を確保しデータの完全性を保証し認証するために必要な鍵を管理し、不認不可保証手段により、セキュリティドメイン内の通信の事実を保証することができる。

【００２２】（２）異種オブジェクト統合管理モデルの

6

採用

異種オブジェクト統合管理モデルの採用により、セキュリティドメイン間にまたがるアクセスを行なうオブジェクトの管理ができる。また、オブジェクト管理の操作手段の提供により、各オブジェクト情報の整合性を確保することができるため、「自己管理」していないシステムでのオブジェクト管理が可能である（図８～図１１）。これらの管理には、前記先願１の異種オブジェクト統合管理方式を利用することができる。

【００２３】（３）セキュリティ管理オペレーションの提供

具体的なセキュリティ管理オペレーションの提供により、システムの管理アプリケーションに情報ＤＢのサービスを利用させることができる（図１２）。

【００２４】以上のようにして、オープン分散環境での管理とセキュリティの解となるモデルにより、アプリケーションやシステム、ネットワーク間に跨がった視点からセキュリティを管理でき、しかも自己管理していないシステムでのオブジェクトが管理でき、さらにシステムの管理アプリケーションのオペレーションを提供することができる。本発明により、現状のネットワークシステムをセキュリティ機能を損なうことなく拡張することができる。

【００２５】

【実施例】以下に、本発明の実施例を図面により説明する。

【００２６】図１は、本発明の一実施例によるセキュリティ管理モデルの適用対象となるネットワークシステムの構成図である。同図で、Ａ，Ｂ，及びＣはセキュリティドメイン（ネットワーク管理システム）、ＮＷ１，…は広域ネットワーク、ＷＳ１，ＷＳ２，……，ＷＳ８はワークステーション、Ｒはルータである。本実施例では、同図に示すような複数の広域ネットワークＮＷ１（図ではその１つを示す）を介して接続される複数のコンピュータシステムに適用される、ネットワークシステム全体のセキュリティを実現するセキュリティ管理モデルを提案している。図１の例では、複数のセキュリティドメインＡ，Ｂ，Ｃからネットワークが構成されており、使用されるワークステーション等の機種は、ドメイン内では原則として同一機種であるが、ドメイン相互間では異なる機種の場合が多くなっている。

【００２７】第１　ネットワーク間に跨がったセキュリティ管理

１．１　セキュリティポリシーの規定

図２は、図１において、本実施例の特徴であるＴＴＰを設け、ＯＳＩ管理ドメインに跨がってセキュリティ管理をするモデルの構成図、図３は図２に対応するＴＴＢの動作の流れ図、図４は図２におけるセキュリティポリシーの表現方法の一例を示す図、図５は図３の一部であるセキュリティポリシーのパラメータ比較方法の一例を示

す流れ図である。分散環境では、ネットワーク間に跨がった分散サービスやアプリケーション、ネットワーク間に跨がって利用されるデバイスをどのように使用させるかという管理をしなければならない。現在のＯＳＩ管理モデルではネットワークマネジャM_A，M_B，M_Cが管理する部分についてはアクセス権限やエンティティの認証が管理されているが、各マネジャの管理範囲を超えた部分については改めてどのようなセキュリティポリシーに基づいてネットワークエンティティのオブジェクト管理をするか決める必要がある。そこで本実施例では、オープン分散環境におけるＯＳＩマネジャの管理範囲を超えた部分については、ＴＴＰ即ち信頼できる第三者に管理させる。

【００２８】図２と図３に示すように、異なるＯＳＩ管理のドメインＡとドメインＢ（なお、以下では、一般化したドメインをｉ，ｊで示すことがある）がある場合、両方のドメインのマネジャ（M_A及びM_B）から信頼されたＴＴＰを設定し、そのＴＴＰにドメインＡとドメインＢの全体のセキュリティポリシーＰを管理させるモデルを提案する。ドメインＡ及びＢは、各々のセキュリティポリシーP_A及びP_BをＴＴＰに登録要求する（①）。すると、ＴＴＰは、ドメインＡのセキュリティポリシーP_AとドメインＢのセキュリティポリシーP_Bを、認証、アクセス制御、完全性、機密性、オーディット（Audit：監査）等のＯＳＩセキュリティフレームワークで規定された観点から比較し、表現が異なる部分についてはマッピングを行うことにより両ドメインのセキュリティポリシーの相違を吸収させ、システム全体として矛盾のないセキュリティポリシーＰを作成する（②）。このセキュリティポリシーＰに基づいてドメインＡとドメインＢの両方にまたがる部分の処理を行なう。

【００２９】前記管理モデルの実現のためには、セキュリティポリシーの表現方法の規定、及び世界的に共通なセキュリティ評価基準が必要であるが、この表現方法及び評価基準（比較方法）の一例を図４及び図５に示す。図４及び図５では、ドメインＡのセキュリティポリシーP_Aを、認証、アクセス制御、完全性、機密性、オーディットの保証要件を示すパラメタで表現している。まず、これらのパラメタP_A，P_Bがシステムの最低要件パラメタP_0より大きいかどうか調べる。大きかった場合には、両ドメインＡ、Ｂのセキュリティポリシーのパラメタと比較して、その小さい方の値（すなわち共通する部分）がセキュリティポリシーＰのパラメタP_0として生成される。

【００３０】図２の管理モデルを実装ベースで考えると、ＴＴＰには複数のネットワーク管理システムのセキュリティポリシーを各ネットワークマネジャと通信しあう管理システムが必要である。例えば図６及び図７にＴＴＰとネットワーク管理システムＡ（ドメインＡ）のマネジャとの間で行なわれるアクセス制御ポリシーに関する設定手段、更新手段の処理の流れを示す。図６のネットワーク管理システムＡ及びネットワーク管理システムＢ（ドメインＢ）は、既にドメイン間に跨がるアクセス制御について各々のセキュリティポリシーP_A及びP_BをＴＴＰに登録済みであるとする。システムＢのマネジャM_BによるポリシーP_Bの変更要求（①）がシステムＡのポリシーP_Aに影響を及ぼす場合（例えば関係属性がある場合など、後述の図１０参照）には、ＴＴＰはシステムＡのマネジャM_Aに対して通知すること（②）が必要である。また、新たにネットワーク管理システムＣのマネジャM_Cが、ドメイン間に跨がるアクセス制御についてセキュリティポリシーP_CをＴＴＰに登録要求（③）する場合には、まずＴＴＰにシステムＣを認証してもらった（④）上で、次にポリシーP_Cの追加がポリシーP_A及びP_Bに影響を及ぼす場合には、ＴＴＰはシステムＡ及びＢのマネジャ（M_A、M_B）に対して通知すること（④）が必要である。

【００３１】一方、実際にドメイン間に跨がるアクセスが発生した場合のアクセス制御確認（判定）手段の例を図８及び図９に示す。図８に示したように、ＴＴＰは、ドメイン間に跨がるアクセス制御についてポリシーP_A、P_B及びP_Cを管理しているため、システムＡのマネジャM_AはオブジェクトａのシステムＢへのアクセス要求の可否についてはＴＴＰに問合せなければならない（①）。ＴＴＰではシステムＡのオブジェクトａの属性とシステムＢのオブジェクトｂの属性（後記図１５，図１６参照）及びポリシーP_A、P_Bを比較することにより、オブジェクトａのアクセス可否を判断し、その結果をM_Aに知らせる（④）。アクセス制御の判断の過程でオブジェクトｂの認証が必要になった場合には、ＴＴＰはシステムＢのマネジャにオブジェクトｂに関する認証情報AI_bを提示させる（②③）。

【００３２】１．２　監査機能の提供

ＴＴＰには、監査機能を備えることによりシステムに対するセキュリティ侵害事象を収集、解析し警告を発するセキュリティ監査手段が必要である。特に、複雑なコンピュータネットワークのメンテナンスやネットワーク装置の再構成に伴い、セキュリティポリシーＰが矛盾なく遂行されることをＴＴＰは確認する。また、ＴＴＰが性能監視や保証（guarantee）機能も提供する。監査機能の実現例を図１０及び図１１に示す。ドメインマネジャM_Aは、システムＡ内で検出したセキュリティ侵害をＴＴＰに報告する（①）。ＴＴＰが前記報告を重要とみなした場合には、セキュリティ侵害に対する警告及び指示をシステムＡ及びＢに対して発行する（②）。

【００３３】１．３　鍵管理機能の提供

複数の管理ドメイン間に跨がったネットワークシステムでのセキュリティ機能のためには、ＴＴＰが鍵管理手段を提供する。ネットワークシステム内での安全な通信を確保するために必要な機密性や完全性機能のためにも、

9

また認証のために発行されるＣｅｒｔｉｆｉｃａｔｅやチケットの配送のためにも鍵管理は不可欠である。ドメインが拡張する度に新しい鍵管理機能を作り直すことにならないように、当初から堅固な鍵管理機構が必要である。鍵管理機能の実現例を図１２及び図１３に示す。ドメインマネジャM_A及びM_Bが発行した鍵要求（①）に対して、ＴＴＰは鍵を作成しシステムＡ及びＢに対して配布する（②）。

【００３４】１．４　否認不可機能の提供

否認不可フレームワークで規定されているような通信の事実を保証する必要がある場合には、ＴＴＰは通信の証拠情報を収集し、必要に応じて提示する必要がある。また、通信の当事者間で解決できず調停を求められた場合には、証拠情報を元に判断を下す必要がある。否認不可保証手段の実現例については本出願人の特許出願に係る特願平５－２６８５９５号（先願２）の「ネットワークシステムの否認不可方式」により提案されており、本実施例ではこの先願２の提案を採用することができる。

【００３５】第２　ＯＳＩ管理ドメイン間に跨がったオブジェクト管理－ＳＮＭＰとの融合

２．１　異なるドメインのオブジェクト管理

各ドメインのセキュリティポリシーは、図２に示した管理モデルに従いオブジェクト化されて管理されているという前提とする。この場合、図２のドメインＡとドメインＢのマネジャM_A及びM_Bは、従来どおり自ドメイン内のオブジェクトの管理を行い、異なるドメインへのアクセスに関してはＴＴＰに問合わせるが、ドメイン間にまたがりアクセスするオブジェクトを新たに管理する必要がある。つまり、図８でのオブジェクトａ及びオブジェクトｂの管理をシステムＡ及びシステムＢでしなければならない。

【００３６】異なるネットワーク管理システムのオブジェクトの統合管理方法の一方式を前記先願１「異種オブジェクト統合管理方式の管理モデル」で提案したが、そこでのオブジェクト管理方法を本実施例によるセキュリティ管理モデルのオブジェクト管理手段に適用する。図１４に示すシステム（No.0）がＴＴＰに相当し、各システム（No.1-n）が各々ＭＩＢ（Management Information Base）を持ちドメイン間にまたがるアクセスを行うオブジェクトを管理する。そして、ＴＴＰのMIB_Tでは前記オブジェクトに関する関係情報（図１５，図１６）を統一的に格納する。図１４のモデルでは、ＴＴＰと各システム間の操作にはＣＭＩＰ（CommonManagemet Information Protcol）を用いるが、ネットワーク管理システムがＳＮＭＰ（Simple Network Management Protcol）であってもＭＩＢさえサポートすればオブジェクト管理ができる。

【００３７】また、オブジェクトａ，ｂ，ｃの関係づけのために関係属性を導入した。図１５は関係属性の例として拡張ピア属性を示す図である。一般にＮ個対Ｎ個の

10

オブジェクト間の関係を示すピア属性（同位属性）を拡張ピア属性という。図１５に示すように、各オブジェクトの情報に相互関係があることを管理するために、オブジェクトａに関係属性値にオブジェクト名称である「ｂ」「ｃ」を指定する。また、同様にオブジェクトｂには「ａ」「ｃ」を、オブジェクトｃには「ａ」「ｂ」を指定する。このように関係属性の値にオブジェクト名称を拡張ピア属性として設定することにより、オブジェクト間を関係付ける。

【００３８】さらに、オブジェクトの情報の整合性合わせのために追加属性を導入した。図１６は追加属性の例としてアクセス属性を示す説明図である。図１６の例では、オブジェクトａの追加属性の値が「２」から「３」に変化すると、拡張ピア関係にあるオブジェクトｂ及びｃの追加属性も「２」から「３」に変化させている。このように、ピア関係で結ばれた各オブジェクトの追加属性の値を等しくするような管理を、セキュリティ管理モデルではＴＴＰが実行する。

【００３９】２．２　オブジェクト管理の操作の提供

セキュリティ管理モデルで、２．１に示したように、各システムがドメイン間に跨がりアクセスするオブジェクトを管理するためには、図１５で示したような各オブジェクトの情報の整合性を確保することが必要である。整合性を確保するためのオブジェクト調整手段として、前記先願１で提案しているオブジェクトの統合管理方法を採用する。図１７はオブジェクトの生成及び削除、並びにオブジェクト情報の更新を行なうオブジェクト調整手段の構成図、図１８は図１７に対応するＴＴＰの動作説明図、図１９は図１７に対応するオブジェクト情報更新時の状態変化を示す図である。図１７に示すように、オブジェクトの生成及び削除、オブジェクト情報の更新時にはＴＴＰと各システム間ではＣＭＩＰに基づく操作を行う。以下に、図１７～図１９により本実施例の動作を説明する。

【００４０】①　システムＡのオブジェクトに生じた事象を、システムＡのエージェント機能部分が検知し、システムＡのマネージャ機能部分にローカルプロトコルを用いて伝送する。

【００４１】②　発生事象をシステムＡはＴＴＰに対して操作要求する。

【００４２】③　ＴＴＰのエージェント機能部分がシステムＡのオブジェクトに生じた事象をＴＴＰのマネージャ機能部分にローカルプロトコルを用いて伝送する。

【００４３】④　ＴＴＰは、事象を検知したオブジェクトと拡張ピア関係で結ばれたオブジェクトをＴＴＰのMIB_Tにより調べ、該当するシステムＢのエージェント機能部分に対して操作要求する。

【００４４】第３　高位なセキュリティ管理オペレーション

システムの管理アプリケーションにＯＳＩ環境で利用さ

11

れるデータや管理情報の転送を行うサービスのための実現例を示す。システムの管理アプリケーションＡＰには、ＴＴＰのＭＩＢ$_T$の管理するセキュリティポリシーＰ及びオブジェクトの情報に基づいて、暗号化、完全性、否認不可というセキュリティ機能を実行させるためにＡＰＩを用いる。図２０は、このセキュリティ実行方法の一例を示す説明図である。図２０の例では、次の処理を行っている。

【００４５】①　システムＡはアプリケーションＡＰ１のシステムＢ内のデータベースＤＢ１に対するアクセス判定をＴＴＰに対して要求する。

【００４６】②　ＴＴＰはＭＩＢ$_T$内の情報を確認し、判定結果をシステムＡの通知する。

【００４７】③　判定結果がＯＫだった場合には、アプリケーションＡＰ１の処理を実行し、データベースＤＢ１対してアクセス要求をする。

【００４８】以上の実施例によれば、オープン分散環境での管理とセキュリティの解となるモデルを提案することにより、今後問題となってくるオープンなネットワークシステムでのセキュリティに対応でき、現状のネットワークシステムをセキュリティ機能を損なうことなく拡張することができるセキュリティ管理装置が得られる。

【００４９】

【発明の効果】以上詳しく説明したように、本発明によれば、オープンな異機種の分散システム環境において、色々な機種をもつ複数のネットワークシステム間に跨がってセキュリティ管理を行なうためにＴＴＰを設け、このＴＴＰ上で、セキュリティポリシーの設定登録、更新を行ない、またこのセキュリティポリシーの規定に従ってネットワークシステム間のアクセスを制御するようにしたので、異機種を有するネットワークシステム間に跨がって発生するアクセス要求に対するセキュリティ管理が容易に確実に実現できるという効果が得られる。また、このＴＴＰ上で、セキュリティ監査手段によりセキュリティ侵害事象を収集解析し警告を発生することができ、鍵管理手段によりネットワークシステム内の安全な通信の確保、データの安全性の保証及び認証のために必要な暗号鍵の管理をすることができ、否認不可保証手段により、ネットワークシステム内の通信の事実を保証することができる等の効果も得られる。

【図面の簡単な説明】

【図１】本発明の一実施例のセキュリティ管理モデルの適用対象となるネットワークシステムの構成図である。

【図２】本発明の一実施例のＯＳＩ管理ドメイン間に跨がったセキュリティ管理モデルの構成図である。

【図３】図２に対応するＴＴＰの動作を示す流れ図である。

【図４】セキュリティポリシーの表現方法の一例を示す図である。

【図５】図３におけるセキュリティポリシーの比較方法の一例を示す図である。

12

【図６】ＴＴＰとネットワーク管理マネジャ間でのアクセス制御についてのセキュリティポリシー設定手段及び更新手段の一例を示す構成図である。

【図７】図６に対応するＴＴＰの動作を示す流れ図である。

【図８】ドメイン間に跨がるアクセスが発生した場合のアクセス制御判定手段の一例を示す図である。

【図９】図８に対応するＴＴＰの動作を示す流れ図である。

【図１０】ＴＴＰが複数の管理ドメイン間に跨がったネットワークシステムに提供するセキュリティ監査手段の一例を示す構成図である。

【図１１】図１０に対応するＴＴＰの動作を示す流れ図である。

【図１２】ＴＴＰが複数の管理ドメインに跨がったネットワークシステムに提供する鍵管理手段の一例を示す構成図である。

【図１３】図１２に対応するＴＴＰの動作を示す流れ図である。

【図１４】オブジェクト統合管理方式の管理モデルを本発明によるセキュリティ管理モデルのオブジェクト管理手段に適用した一例を示す図である。

【図１５】オブジェクト間の関係付けのために導入した拡張ピア属性を説明する図である。

【図１６】オブジェクトの情報の整合性合わせのために導入した追加属性を説明する図である。

【図１７】オブジェクトの生成及び削除、並びにオブジェクト情報の更新を行なうオブジェクト調整手段の一例を示す図である。

【図１８】図１７に対応するＴＴＰの動作を示す説明図である。

【図１９】図１７に対応するオブジェクト情報更新時の状態変化を示す図である。

【図２０】システムの管理アプリケーションにセキュリティ機能を実行させる一例を示す図である。

【符号の説明】

Ａ，Ｂ，Ｃ　ネットワーク管理システム（ドメイン）

AI_b　オブジェクトｂの認証情報

ＡＰ１　アプリケーション

Ａｕ，Ａｃ，Ｉｎ，Ｃｎ，Ａｄ　セキュリティポリシーの保証要件を示すパラメタ

ａ，ｂ，ｃ，ｘ　オブジェクト

ａ→Ｂ　オブジェクトａのシステムに対するアクセス判定要求

ＤＢ１　データベース

M_A，M_B，M_C　各ドメインのマネジャ

ＭＩＢ　Ｍａｎａｇｅｍｅｎｔ　Ｉｎｇｏｒｍａｔｉｏｎ　Ｂａｓｅ

MIB_A，MIB_B，MIB_C　ネットワーク管理システ

13

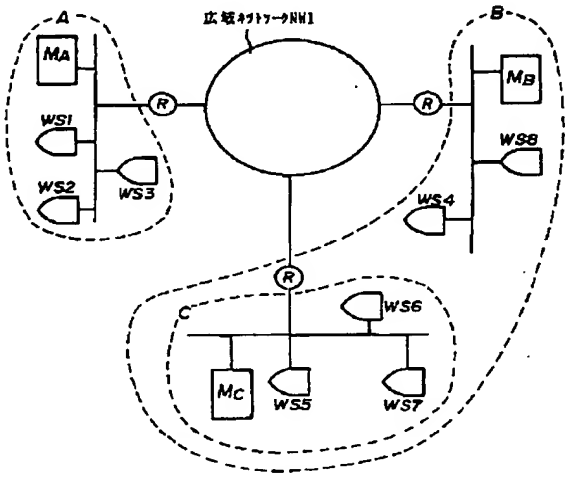
ムA，B，CのMIB
MIB，TTPのMIB
NW1　ネットワーク
P　セキュリティポリシー
P_A，P_B，P_C　各ドメインのセキュリティポリシー
P_0　システムのセキュリティ機能の最低要件を示すパ

14

ラメタ
R　ルータ
TTP　Trusted　Third　Party（信頼できる第三者）
WS1～WS8　ワークステーション

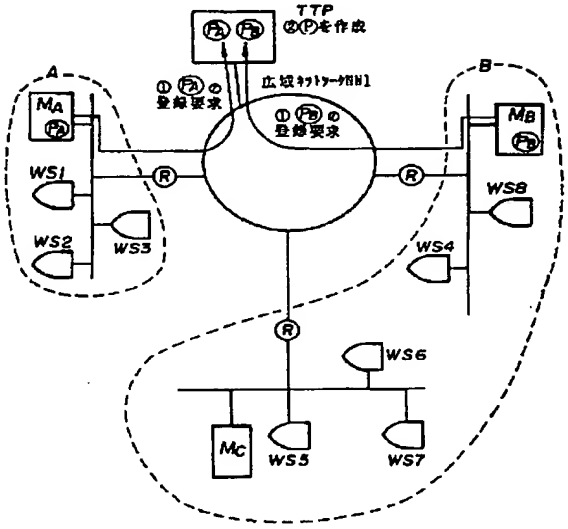
【図1】

【図 1】 セキュリティ管理モデルの適用対象となるネットワークシステム



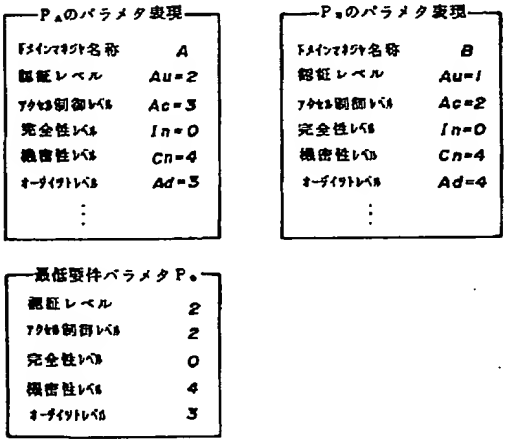
【図2】

【図 2】 OSI管理ドメイン間に跨がったセキュリティ管理モデル



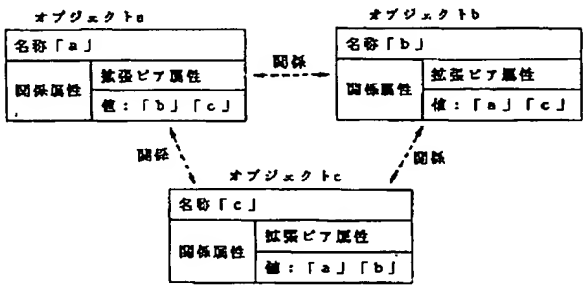
【図4】

【図 4】 セキュリティポリシーの表現方法



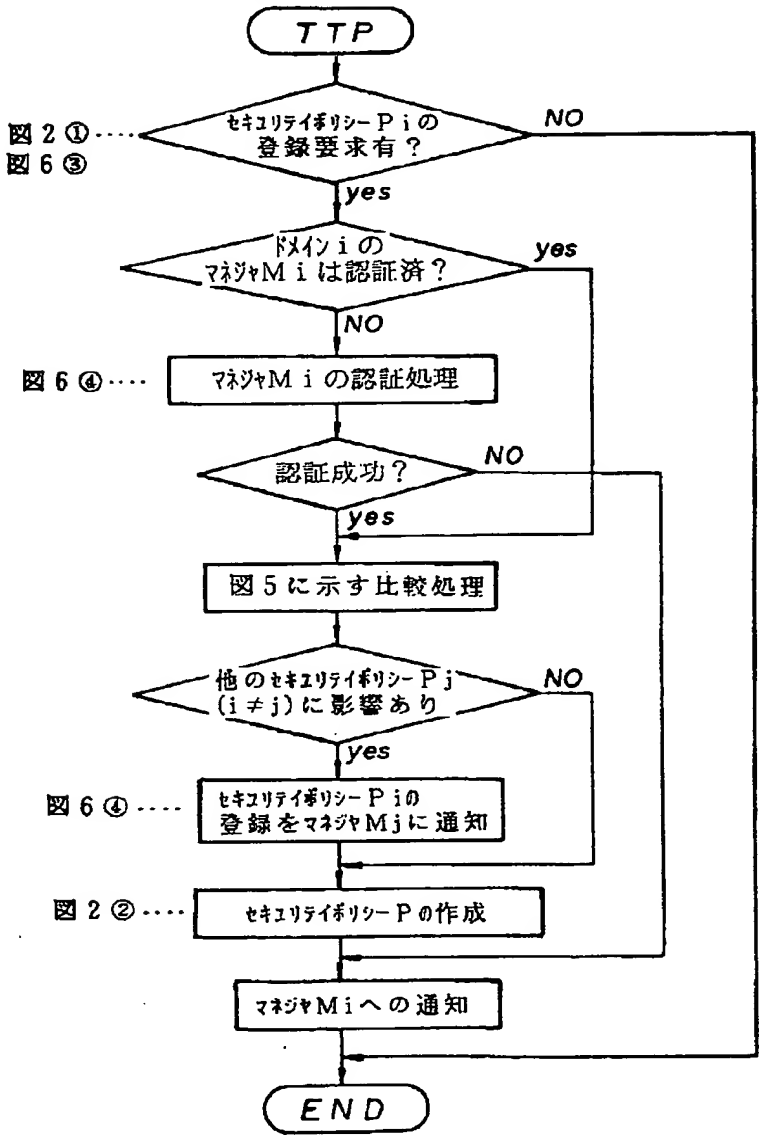
【図15】

【図 15】 拡張ピア属性



【図3】

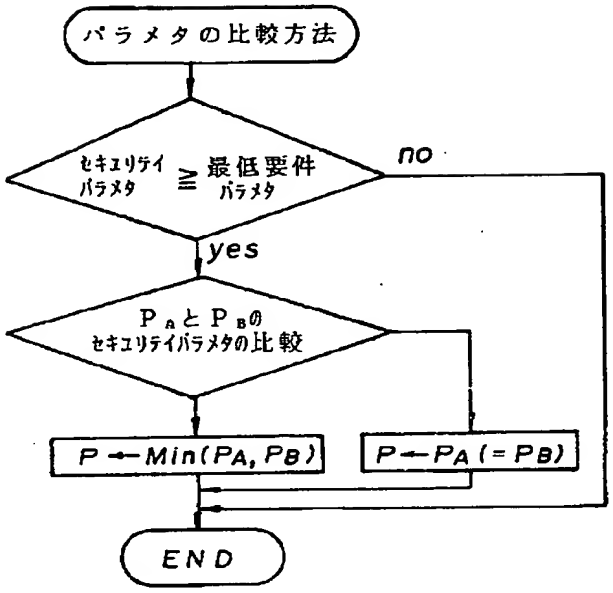
【図 3 】図2に対応するＴＴＰの動作



【図5】

【図５】

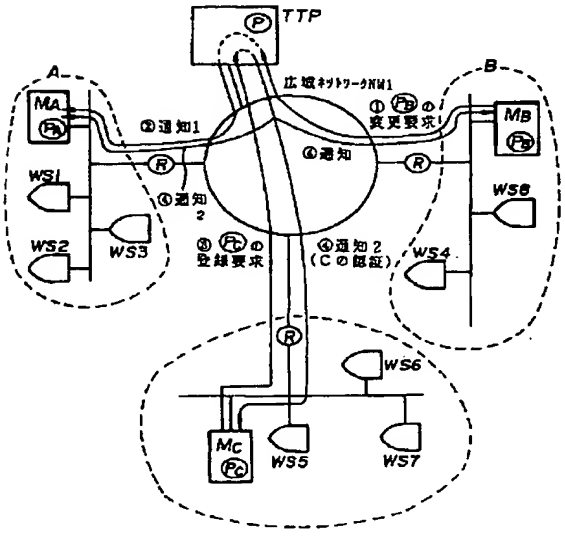
セキュリティポリシーの比較方法



【図6】

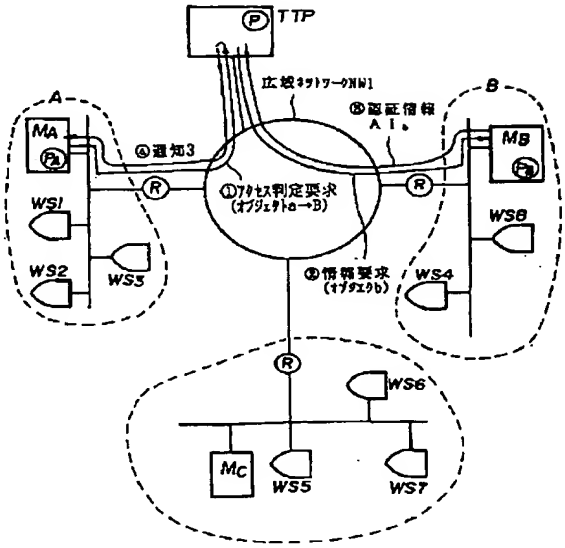
【図６】

セキュリティポリシー設定手段，更新手段



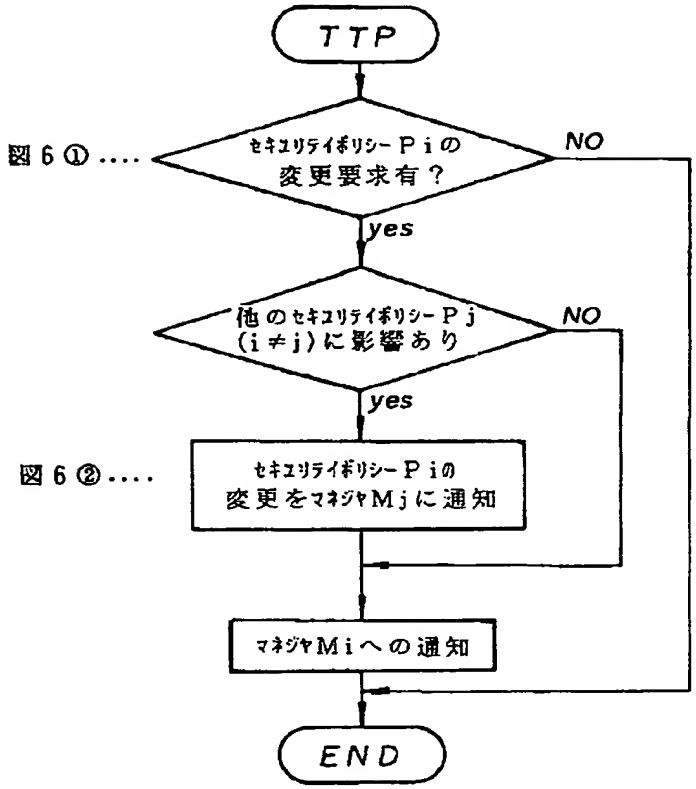
【図8】

【図８】 アクセス制御判定手段



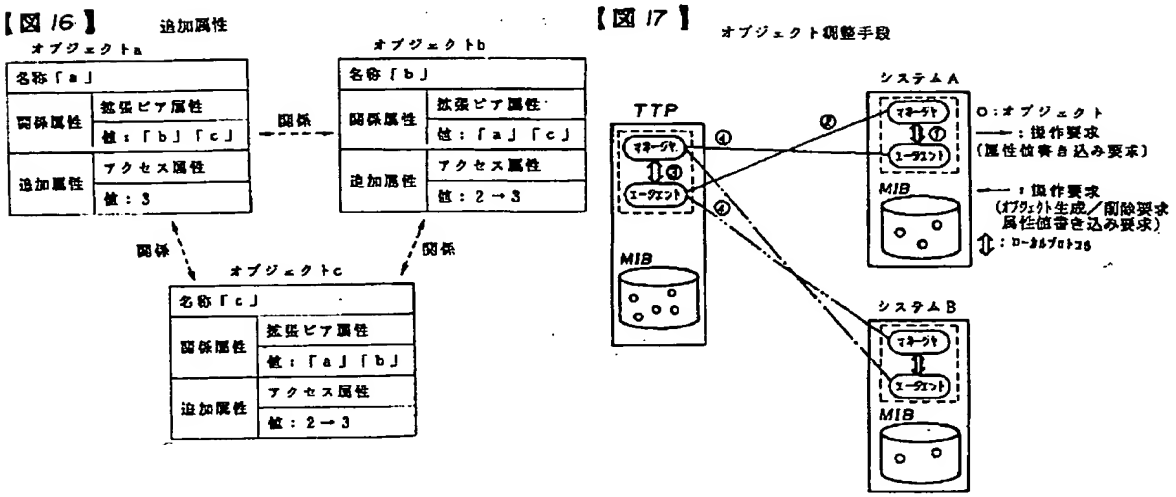
【図７】

【図７】図６に対応するＴＴＰの動作



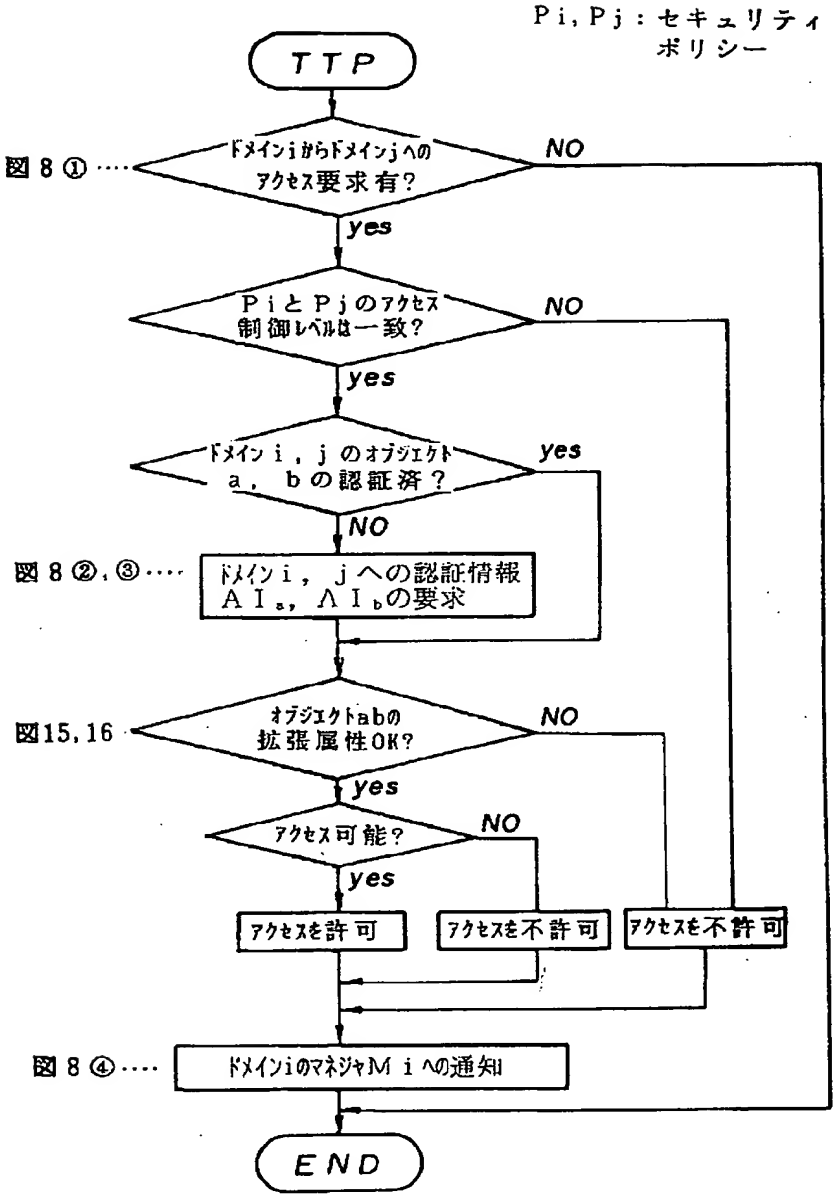
【図１６】

【図１７】



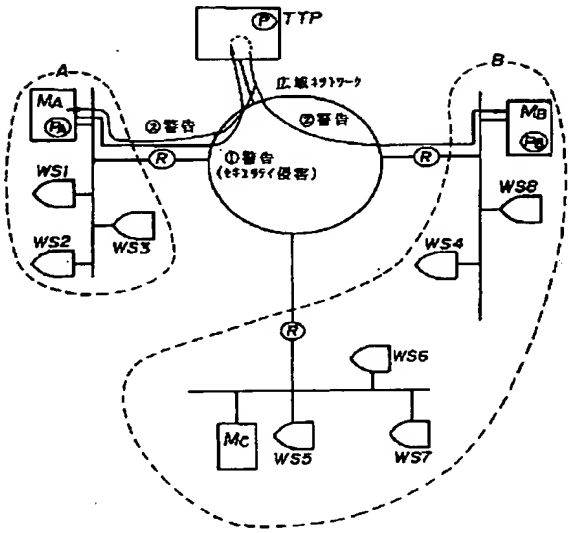
【図9】

【図 9 】図8に対応するＴＴＰの動作



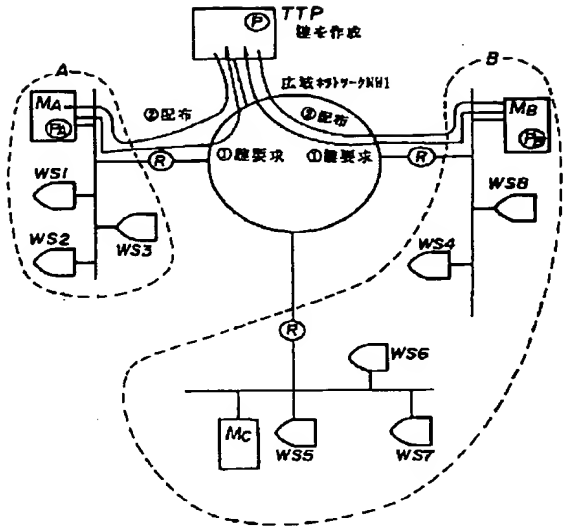
【図１０】

【図 10】 セキュリティ監査手段



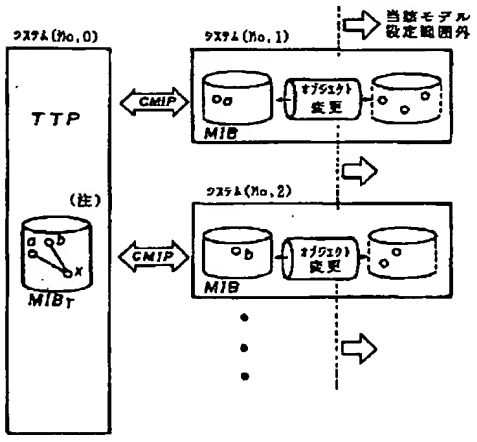
【図１２】

【図 12】 鍵管理手段



【図１４】

【図 14】
セキュリティ管理モデルのオブジェクト管理手段

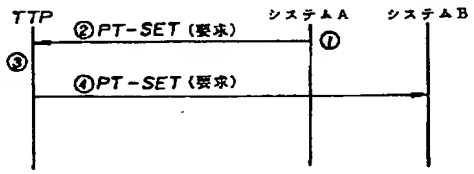


○:オブジェクト

(注) ＴＴＰのＭＩＢは、a,b,x の関係のみ管理する

【図１８】

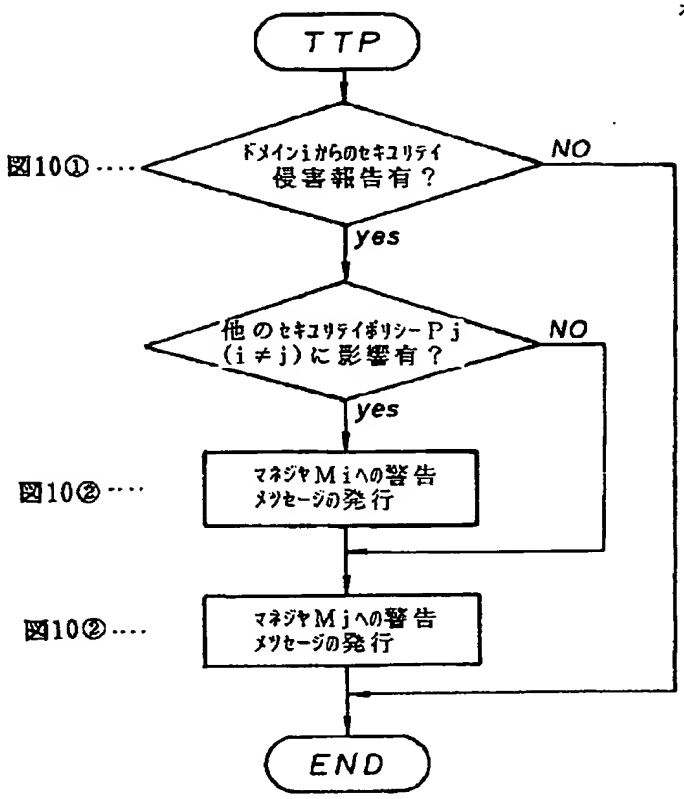
【図 18】
図１７に対応するＴＴＰの動作



【図１１】

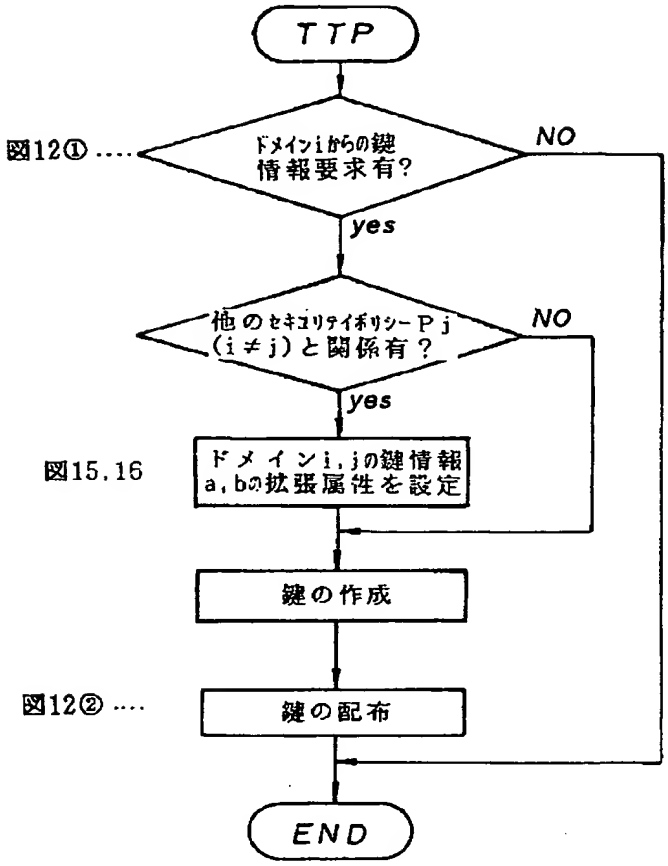
【図 11】図１０に対応するＴＴＰの動作

Ｐｉ，Ｐｊ：セキュリティ
ポリシー



【図１３】

【図 13】 図１２に対応するＴＴＰの動作



【図19】

【図19】

オブジェクト情報更新時の状態変化

	オブジェクトa			オブジェクトb			発生事象
	存在有無	関係属性値	<n>属性値	存在有無	関係属性値	<n>属性値	
TTP MIBの情報	あり ③ なし	b ③ b	s ③ t	あり ③ あり	a ③ a	s ③ t	①システムAのMIBのオブジェクトaの持つ<n>属性値を"s"から"t"に変更要求 ④システムBのMIBの属性値を変更
システムA MIBの情報	あり ① あり	なし ① なし	s ① t	該当せず	該当せず	該当せず	
システムB MIBの情報	該当せず	該当せず	該当せず	あり ④ あり	a ④ a	s ④ t	

上　段 ⇐初期状態
↓
下　段 ⇐最終状態

【図20】

【図20】

システムの管理アプリケーションのセキュリティ機能